ỦY BAN NHÂN DÂN TỈNH AN GIANG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 49 /2013/QĐ-UBND	*An Giang, ngày 31 tháng 12 năm 2013*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn thông tin số trên môi trường mạng trong hoạt động của cơ quan nhà nước trên địa bàn tỉnh An Giang

ỦY BAN NHÂN DÂN TỈNH AN GIANG

Căn cứ Luật Tổ chức Hội đồng nhân dân và Uỷ ban nhân dân ngày 26 tháng 11 năm 2003;

Căn cứ Luật Ban hành văn bản quy phạm pháp luật của Hội đồng nhân dân và Ủy ban nhân dân ngày 03 tháng 12 năm 2004;

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;

Căn cứ Luật Giao dịch Điện tử ngày 29 tháng 11 năm 2005;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về Ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Nghị định số 72/2013/NĐ-CP ngày 15 tháng 7 năm 2013 của Chính phủ về Quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng;

Căn cứ Nghị định số 174/2013/NĐ-CP ngày 13 tháng 11 năm 2013 của Chính phủ quy định xử phạt hành chính trong lĩnh vực bưu chính, viễn thông, công nghệ thông tin và tần số vô tuyến điện;

Căn cứ Thông tư Liên tịch số 06/2008/TTLT-BTTTT-BCA ngày 28 tháng 11 năm 2008 của Liên Bộ Thông tin và Truyền thông, Bộ Công an Về bảo đảm an toàn cơ sở hạ tầng và an ninh thông tin trong hoạt động bưu chính, viễn thông và công nghệ thông tin;

Căn cứ Thông tư số 23/2011/TT-BTTTT ngày 11 tháng 8 năm 2011 của Bộ Thông tin và Truyền thông quy định về việc quản lý vận hành, sử dụng và bảo đảm an toàn thông tin trên Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;

Căn cứ Thông tư số 25/2010/TT-BTTTT ngày 15 tháng 11 năm 2010 của Bộ Thông tin và Truyền thông quy định việc thu thập, sử dụng, chia sẻ thông tin cá nhân và các biện pháp bảo đảm an toàn và bảo vệ thông tin cá nhân trên trang thông tin điện tử hoặc cổng thông tin điện tử của cơ quan nhà nước;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 62/TTr-STTTT ngày 18 tháng 12 năm 2013,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin số trong hoạt động của cơ quan nhà nước trên địa bàn tỉnh An Giang.

Điều 2. Quyết định này có hiệu lực thi hành sau 10 ngày kể từ ngày ký.

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh, Giám đốc Sở Thông tin và Truyền thông, Giám đốc các Sở, Ban, Ngành, Chủ tịch Ủy ban nhân dân các huyện, thị xã, thành phố có trách nhiệm thi hành Quyết định này./.

***Nơi nhận*:**
- VP. Chính phủ (HN - TPHCM);
- Bộ Thông tin và Truyền thông;
- Cục Kiểm tra văn bản - Bộ Tư pháp;
- TT: TU, HĐND tỉnh;
- Chủ tịch và các PCT. UBND tỉnh;
- VP.TU, các Ban đảng;
- UBMTTQ, các đoàn thể tỉnh;
- Như Điều 3;
- Cơ quan Báo, Đài tỉnh;
- Công báo tỉnh;
- Cổng thông tin điện tử tỉnh;
- Lưu: VT.

TM. ỦY BAN NHÂN DÂN TỈNH
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Hồ Việt Hiệp

ỦY BAN NHÂN DÂN TỈNH AN GIANG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc

QUY CHẾ
Bảo đảm an toàn thông tin số trên môi trường mạng trong hoạt động của cơ quan nhà nước trên địa bàn tỉnh An Giang

(Ban hành kèm theo Quyết định số: 49 /2013/QĐ-UBND ngày 31 tháng 12 năm 2013 của Ủy ban nhân dân tỉnh An Giang)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về công tác bảo đảm an toàn thông tin số; trách nhiệm của tổ chức, cá nhân trong hoạt động ứng dụng công nghệ thông tin trên môi trường mạng của các cơ quan Nhà nước trên địa bàn tỉnh An Giang.

Điều 2. Đối tượng áp dụng

1. Quy chế này áp dụng đối với tất cả cán bộ, công chức, viên chức (sau đây gọi tắt là CBCC-VC), các cơ quan Nhà nước (CQNN) trên địa bàn tỉnh An Giang.

2. Tổ chức, cá nhân bên ngoài có liên quan khi tham gia sử dụng hệ thống thông tin của cơ quan nhà nước, để giao tiếp, cung cấp và trao đổi thông tin số với cơ quan nhà nước;

3. Khuyến khích các cơ Đảng, Đoàn thể, Tổ chức Chính trị-xã hội áp dụng quy chế này trong hoạt động ứng dụng công nghệ thông tin (CNTT).

Điều 3. Giải thích từ ngữ

Trong Quy chế này, các từ ngữ dưới đây được hiểu như sau:

1. Phần mềm quản lý văn bản và chỉ đạo điều hành trên môi trường mạng: theo khoản 4 Điều 2 Quyết định số 10/2012/QĐ-UBND ngày 18 tháng 6 năm 2012 của UBND tỉnh An Giang về việc ban hành quy chế sử dụng Hệ thống phần mềm quản lý văn bản và điều hành trên môi trường mạng trong cơ quan nhà nước trên địa bàn tỉnh An Giang.

2. Bảo đảm an toàn thông tin số: Là đảm bảo tính tin cậy, tính toàn vẹn và tính sẵn sàng của thông tin số, trong đó:

a) Tính tin cậy: Đảm bảo thông tin chỉ có thể được truy cập bởi những người được cấp quyền sử dụng.

b) Tính toàn vẹn: Bảo vệ sự chính xác và đầy đủ của thông tin, thông tin không bị sửa đổi làm sai lệch nội dung.

c) Tính sẵn sàng: Thông tin cung cấp được tới đối tượng sử dụng có thẩm quyền đối với thông tin khi có nhu cầu.

3. Trao đổi dữ liệu điện tử (EDI - electronic data interchange): theo khoản 15 Điều 4 Luật Giao dịch điện tử số 51/2005/QH11 ngày 29 tháng 11 năm 2005.

4. Tài khoản người dùng (User Account): theo khoản 8 Điều 2 Quyết định số 10/2012/QĐ-UBND ngày 18 tháng 6 năm 2012 của UBND tỉnh An Giang về việc ban hành quy chế sử dụng Hệ thống phần mềm quản lý văn bản và điều hành trên môi trường mạng trong cơ quan nhà nước trên địa bàn tỉnh An Giang.

5. Mạng nội bộ (LAN - Local Area Networks): là mạng máy tính được thiết lập bằng cách kết nối các máy tính trong cùng một cơ quan, đơn vị cùng một trụ sở, nhằm chia sẻ tài nguyên, thiết bị dùng chung (như tập tin, máy in, máy quét...);

6. Mạng diện rộng (WAN) của tỉnh: là mạng máy tính được thiết lập bằng cách kết nối giữa Trung tâm Tích hợp dữ liệu tỉnh An Giang (Trung tâm Tin học - Sở Thông tin và Truyền thông) với các mạng LAN của các cơ quan, đơn vị thông qua mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;

7. Mạng truyền số liệu chuyên dùng của các cơ quan Đảng và Nhà nước (MTSLCD): là mạng truyền dẫn tốc độ cao, sử dụng phương thức chuyển mạch nhãn đa giao thức trên nền giao thức liên mạng (IP/MPLS) sử dụng riêng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan Đảng và Nhà nước do Tập đoàn Bưu chính Viễn thông Việt Nam xây dựng, vận hành;

8. Mạng Internet: là mạng máy tính toàn cầu, kết nối tới rất nhiều máy tính và mạng máy tính con trên toàn thế giới.

9. Hệ thống thông tin: theo khoản 20 Điều 3 Nghị định số 72/2013/NĐ-CP ngày 15 tháng 7 năm 2013 của Chính phủ về Quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng;

10. Ứng cứu sự cố mạng và an toàn thông tin: Là hoạt động nhằm xử lý, khắc phục sự cố gây mất an toàn thông tin trên hệ thống thông tin.

11. Ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước: theo khoản 1 Điều 3 Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

12. Cơ sở dữ liệu (database): là một hệ thống các thông tin có cấu trúc hoặc không cấu trúc được lưu trữ trên các thiết bị lưu trữ thứ cấp (băng từ, đĩa từ…) nhằm thoả mãn yêu cầu khai thác thông tin đồng thời của nhiều người sử dụng hay nhiều chương trình, phần mềm ứng dụng với nhiều mục đích khác nhau;

13. Phần mềm hệ thống: theo khoản 2 Điều 3 Nghị định số 71/2007/NĐ-CP ngày 03 tháng 5 năm 2007 của Chính phủ quy định chi tiết và hướng dẫn một số điều của Luật Công nghệ thông tin về công nghiệp công nghệ thông tin;

14. Phần mềm ứng dụng: theo khoản 3 Điều 3 Nghị định số 71/2007/NĐ-CP ngày 03 tháng 5 năm 2007 của Chính phủ quy định chi tiết và hướng dẫn một số điều của Luật Công nghệ thông tin về công nghiệp công nghệ thông tin;

15. Máy chủ (Server): là máy tính được kết nối với hệ thống mạng LAN, WAN hoặc mạng internet, có năng lực xử lý cao, trên đó cài đặt các phần mềm để phục vụ cho các máy tính khác truy cập, yêu cầu cung cấp các dịch vụ hoặc cơ sở dữ liệu.

Điều 4. CBCC-VC chuyên trách CNTT

1. Phẩm chất và năng lực CBCC-VC chuyên trách CNTT:

a) Có phẩm chất tốt, có tinh thần trách nhiệm, ý thức tổ chức kỷ luật, ý thức cảnh giác giữ gìn an toàn thông tin.

b) Được đào tạo trình độ cao đẳng trở lên chuyên ngành về Công nghệ thông tin, Lý tin hoặc Toán tin và các ngành tương đương tại các cơ sở giáo dục thuộc hệ thống giáo dục quốc dân hoặc tại các cơ sở giáo dục hợp pháp ở nước ngoài.

2. CBCC-VC chuyên trách CNTT có năng lực đáp ứng khoản 1 Điều này và được phân công:

a) Trực tiếp thực hiện nhiệm vụ chuyên môn công nghệ thông tin, bao gồm các công việc sau:

- Trực tiếp tham gia xây dựng các ứng dụng công nghệ thông tin như: Cổng/Trang thông tin điện tử, phần mềm ứng dụng, cơ sở dữ liệu,…;

- Trực tiếp tham gia vận hành, duy trì và khắc phục các sự cố hệ thống hạ tầng kỹ thuật, phần mềm ứng dụng, cơ sở dữ liệu (CSDL), Cổng/Trang thông tin điện tử; vận hành hệ thống bảo đảm an toàn, an ninh thông tin, …;

b) Không trực tiếp thực hiện nhiệm vụ theo điểm a khoản 2 Điều này, nhưng trực tiếp tham gia quản lý nhà nước về ứng dụng và phát triển công nghệ thông tin tại các cơ quan, đơn vị chuyên trách về công nghệ thông tin.

Điều 5. Nguyên tắc chung về bảo đảm an toàn thông tin số

1. Các cơ quan, tổ chức, cá nhân và CBCC-VC chịu trách nhiệm trước pháp luật về nội dung thông tin đã chuyển đi trên mạng nội bộ (LAN), mạng truyền số liệu chuyên dùng của các cơ quan Đảng và Nhà nước (mạng WAN) và mạng Internet.

2. Bảo đảm an toàn hệ thống thông tin trong hoạt động của cơ quan nhà nước;

3. Tuân thủ các nguyên tắc, các tiêu chuẩn, quy chuẩn kỹ thuật về bảo mật, an toàn thông tin số;

4. Kết hợp nhiều biện pháp bảo đảm an toàn thông tin số, nhằm phát hiện và ngăn chặn kịp thời các nguy cơ mất an toàn, an ninh thông tin;

5. Khi xảy ra sự cố về an toàn thông tin trong hoạt động của cơ quan nhà nước trên địa bàn tỉnh, cần tiến hành các biện pháp khắc phục nhanh chóng, hạn chế thiệt hại tại đơn vị, đồng thời lập biên bản báo cáo theo mẫu Phụ lục I, gửi về Sở Thông tin và Truyền thông.

Điều 6. Các hành vi nghiêm cấm

1. Lưu trữ, dự thảo trên máy tính kết có nối mạng (Internet, Intranet, WAN, LAN) văn bản, tin, tài liệu, số liệu thuộc bí mật Nhà nước hoặc những thông tin, tài liệu mật khác do pháp luật nước Cộng hoà Xã hội Chủ nghĩa Việt Nam quy định;

2. Các hành vi phá hoại, sử dụng các phương tiện kỹ thuật gây nguy hại cho hệ thống thông tin, làm rối loạn, tê liệt một phần hoặc toàn bộ hệ thống thông tin của các cơ quan Nhà nước;

3. Truy cập, khai thác, sử dụng, phát tán, thay đổi, phá hủy các thông tin số thuộc sở hữu của các cá nhân, tổ chức khác khi chưa được phép của chủ sở hữu;

4. Tạo ra, cài đặt, phát tán vi rút máy tính vào máy tính, mạng LAN, mạng truyền số liệu chuyên dùng của các cơ quan Đảng và Nhà nước;

5. Truy cập vào các trang thông tin điện tử trên Internet bị cấm truy cập như: hoạt động xâm phạm an ninh quốc gia, trật tự an toàn xã hội, vi phạm thuần phong mỹ tục, bản sắc văn hoá Việt Nam, xâm phạm các quyền và lợi ích hợp pháp của tổ chức, cá nhân, ... và các trang thông tin điện tử khác trên Internet bị cấm truy cập;

6. Xóa bỏ, làm mất tác dụng của các phần mềm bảo đảm an toàn, an ninh thông tin số được cài đặt trên thiết bị số; tự ý thay đổi các tham số cài đặt của thiết bị số;

7. Ngăn chặn việc truy nhập đến thông tin của tổ chức, cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép;

8. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã, thông tin của tổ chức và cá nhân khác trên môi trường mạng;

9. Tổ chức, cá nhân, CBCC-VC che giấu tên của mình hoặc giả mạo tên của tổ chức, cá nhân khác khi gửi thông tin trên môi trường mạng LAN, mạng truyền số liệu chuyên dùng của các cơ quan Đảng và Nhà nước;

10. Lợi dụng chức vụ, quyền hạn trong quản lý nhà nước về an ninh thông tin số để gây cản trở hoạt động hợp pháp của các chủ thể tham gia hệ thống mạng LAN, mạng truyền số liệu chuyên dùng của các cơ quan Đảng và Nhà nước, tham gia dịch vụ hành chính công trên Internet; xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức và công dân;

11. Các hành vi bị nghiêm cấm tại Điều 12 Luật Công nghệ thông tin; các hành vi khác do các cơ quan quản lý nhà nước quy định nội bộ và pháp luật cấm.

Chương II
GIẢI PHÁP BẢO ĐẢM AN TOÀN THÔNG TIN SỐ

Điều 7. Các giải pháp vận hành bảo đảm an toàn thông tin số

1. Công tác bảo đảm an toàn thông tin số

a) Đối với các cơ quan nhà nước:

- Trang bị đầy đủ các kiến thức bảo mật cơ bản cho CBCC-VC trước khi cho phép truy nhập và sử dụng hệ thống thông tin;

- Phân công CBCC-VC chuyên trách CNTT, để quản lý kỹ thuật nghiệp vụ về an toàn thông tin tại đơn vị;

- Thủ trưởng đơn vị tạo điều kiện CBCC-VC chuyên trách CNTT học tập, tiếp thu công nghệ, kiến thức an toàn thông tin;

- Các cá nhân đã chấm dứt hợp đồng, thôi việc, chuyển công tác, … tiến hành hủy các quyền truy cập hệ thống thông tin; thu hồi hoặc hủy các tài sản liên quan tới hệ thống thông tin nếu có (khóa, thẻ nhận dạng,…); đảm bảo việc chuyển đầy đủ quyền truy cập

thông tin, dữ liệu số từ các tài khoản cá nhân nêu trên, đến cá nhân khác được giao nhiệm vụ thay thế;

- Hàng năm, xác định các nhiệm vụ bảo đảm an toàn thông tin hệ thống (mở rộng, nâng cấp trang thiết bị; đào tạo, bồi dưỡng kiến thức CNTT, ...), để đề xuất kinh phí đến cơ quan có thẩm quyền hoặc phân bổ kinh phí duy trì hoạt động hệ thống thông tin hiệu quả.

b) Nguồn kinh phí thực hiện nhiệm vụ chuyên môn thuộc công tác bảo đảm an toàn, an ninh thông tin do ngân sách nhà nước bảo đảm, theo quy định của Luật Ngân sách nhà nước và các văn bản pháp luật khác có liên quan.

2. Các giải pháp cơ bản đảm bảo trong vận hành an toàn hệ thống:

a) Hệ thống bảo vệ máy chủ đảm bảo chống sét, hệ thống làm mát,…; đảm bảo cung cấp nguồn điện hoạt động liên tục và ổn định.

b) Quản lý các tài khoản của hệ thống thông tin, tài khoản người dùng bao gồm: Tạo mới, sửa đổi, hủy các tài khoản. Thường xuyên kiểm tra các tài khoản của hệ thống thông tin; triển khai các công cụ để hỗ trợ việc quản lý các tài khoản của hệ thống thông tin;

c) Hệ thống thông tin giới hạn tối đa 03 (ba) lần đăng nhập liên tiếp sai tài khoản người dùng, hệ thống tự động khóa tài khoản hoặc cô lập tài khoản trong một khoảng thời gian nhất định, để được đăng nhập hệ thống thông tin lần kế tiếp;

d) Kiểm soát và theo dõi tất cả các phương pháp truy cập từ xa tới hệ thống thông tin, triển khai nhiều cơ chế giám sát, cam kết từ các truy cập từ xa; phát hiện sớm việc truy cập trái phép vào mạng máy tính hay thiết bị lưu trữ dữ liệu;

đ) Giám sát, kiểm tra truy cập không dây, sử dụng chứng thực, mã hóa để bảo vệ truy cập không dây tới hệ thống thông tin;

e) Thiết lập hệ thống thông tin ghi nhận và lưu vết các sự kiện: Quá trình đăng nhập hệ thống, các thao tác cấu hình hệ thống, quá trình truy xuất hệ thống,...Ghi nhận đầy đủ các thông tin trong các bản ghi nhật ký, thời gian lưu trữ các bản ghi nhật ký hệ thống tối thiểu 01 năm;

g) Cập nhật và lưu trữ cấu hình chuẩn các thành phần của hệ thống, trước khi tiến hành cài đặt, thiết lập cấu hình lại hệ thống thông tin, đảm bảo duy trì hoạt động của hệ thống thông tin; Kiểm soát quá trình cài đặt trên máy chủ;

h) Cấu hình hệ thống thông tin cung cấp những chức năng cơ bản cho người dùng; thiết lập các chế độ phân quyền truy cập theo chỉ đạo của Thủ trưởng đơn vị;

i) Định kỳ sao lưu (backup) thông tin, dữ liệu của đơn vị và lưu trữ thông tin sao lưu ở nơi an toàn theo quy định; thường xuyên kiểm tra thông tin, dữ liệu sao lưu để đảm bảo tính sẵn sàng và toàn vẹn;

k) Triển khai cơ chế phòng, chống vi rút máy tính, các sự cố do tấn công mạng, như: cài đặt tường lửa (firewall), phần mềm diệt vi rút máy tính,....

l) Sử dụng mật khẩu: đặt cho tài khoản sử dụng ở dạng phức tạp (bao gồm chữ hoa, chữ thường trong bảng chữ cái, số hoặc các ký tự đặc biệt), độ dài tối thiểu 8 ký tự. Không tiết lộ, chia sẻ mật khẩu cho người khác, khi kết thúc công việc hoặc chuyển giao máy tính cho người khác sử dụng phải thoát khỏi tài khoản người dùng.

Điều 8. Xây dựng quy chế bảo đảm an toàn thông tin nội bộ

Trên cơ sở quy chế này và hướng dẫn của Bộ, Ngành Trung ương, từng CQNN, ban hành quy chế bảo đảm an toàn thông tin nội bộ, quy định rõ các vấn đề cơ bản sau:

1. Phân công cụ thể CBCC-VC chuyên trách CNTT, số điện thoại liên hệ khi có sự cố về an toàn thông tin;

2. Phân công CBCC-VC chịu trách nhiệm quản lý máy tính để dự thảo các văn bản, tài liệu có tính mật; việc sử dụng và vận hành máy tính này, đảm bảo tuân thủ các quy định của pháp luật về bảo mật và an toàn thông tin;

3. Thiết lập quy tắc vào ra, quản lý phòng máy chủ; quy tắc cài đặt phần mềm lên máy chủ, máy tính trạm;

4. Quy tắc phân loại và quản lý mức độ ưu tiên đối với các tài nguyên của hệ thống thông tin (phần mềm, dữ liệu, trang thiết bị…);

5. Kiểm tra, rà soát và khắc phục sự cố an toàn an ninh của hệ thống thông tin sử dụng các biện pháp trong Điều 7 của Quy chế này;

6. Quy tắc quản lý bảo đảm an toàn hệ thống thông tin tại đơn vị; đảm bảo tính toàn vẹn, tính tin cậy, tính thống nhất và tính sẵn sàng của dữ liệu trong quản lý và vận hành trao đổi thông tin.

7. Quy trình xử lý các sự cố ảnh hưởng đến an toàn, an ninh hệ thống tại đơn vị;

8. Chế độ báo cáo tổng hợp tình hình an toàn, an ninh của hệ thống thông tin.

Điều 9. Quy trình phối hợp ứng cứu sự cố mạng bảo đảm an toàn thông tin số trên địa bàn tỉnh

1. Quy trình xử lý khẩn cấp

Khi phát hiện hệ thống có nguy cơ mất an toàn như: hệ thống hoạt động chậm bất thường, không truy cập được hệ thống ứng dụng, nội dung cổng/trang thông tin điện tử hoặc giao diện ứng dụng bị thay đổi, thực hiện các bước cơ bản:

a) Bước 1: Ngắt kết nối máy chủ ra khỏi hệ thống mạng, báo cáo sự cố đến Thủ trưởng đơn vị, thông báo đến Sở Thông tin và Truyền thông, doanh nghiệp cung cấp hạ tầng viễn thông để hỗ trợ khắc phục;

b) Bước 2: Sao chép nhật ký truy cập của người dùng (logfile) và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ (phục vụ cho công tác phân tích);

c) Bước 3: Khôi phục lại hệ thống, hoặc sử dụng hệ thống dự phòng và chuyển dữ liệu sao lưu dự phòng (backup) mới nhất để hệ thống hoạt động;

2. Nguyên tắc phối hợp trong ứng cứu sự cố

a) Các đơn vị thực hiện khắc phục các bước ban đầu theo quy chế bảo đảm an toàn thông tin nội bộ.

b) Các sự cố vượt quá khả năng xử lý của đơn vị, lập biên bản ghi nhận và thông báo đến Sở Thông tin và Truyền thông qua thư điện tử (email) sotttt@angiang.gov.vn và ttth@angiang.gov.vn; tùy theo thời điểm và cán bộ phụ trách, Sở Thông tin và Truyền

thông sẽ có thông báo số điện thoại để thông báo sự cố; Sở Thông tin và Truyền thông sẽ phối hợp giữa các tổ chức, doanh nghiệp liên quan để khắc phục sự cố;

c) Sở Thông tin và Truyền thông báo cáo về Ủy ban nhân dân tỉnh đồng thời thông báo đến Bộ Thông tin và Truyền thông thông qua Trung tâm Ứng cứu khẩn cấp Máy tính Việt Nam, để được hỗ trợ khắc phục các sự cố vượt quá khả năng xử lý của địa phương.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN SỐ

Điều 10. Trách nhiệm của tổ chức, cá nhân bên ngoài khi tham gia sử dụng hệ thống thông tin của cơ quan nhà nước, để giao tiếp, cung cấp và trao đổi thông tin số với cơ quan nhà nước

1. Nghiêm chỉnh thi hành quy chế này và các quy định khác của pháp luật về bảo đảm an toàn thông tin số.

2. Khi phát hiện sự cố ảnh hưởng đến an toàn, an ninh hệ thống thông tin, phải thông báo ngay với cơ quan Nhà nước, nơi tổ chức, cá nhân đang thực hiện giao tiếp.

Điều 11. Trách nhiệm của CBCC-VC trong cơ quan nhà nước

1. Nghiêm chỉnh thi hành quy chế này và các quy định khác của pháp luật về bảo đảm an toàn, an ninh thông tin.

2. Khi phát hiện sự cố ảnh hưởng đến an toàn, an ninh hệ thống thông tin, phải thông báo ngay với đến CBCC-VC chuyên trách CNTT của đơn vị.

3. Các thông tin, tài liệu, văn bản có tính mật theo quy định, phải dự thảo, lưu trữ đúng theo quy định về bảo bảo mật và an toàn thông tin.

4. CBCC-VC chuyên trách CNTT:

a) Triển khai hoặc tham mưu để triển khai thực hiện các nội dung tại Khoản 2 Điều 7 và Điều 9 Quy chế này;

b) Theo nhiệm vụ được Thủ trưởng đơn vị phân công, chịu trách nhiệm tham mưu chuyên môn và vận hành đảm bảo an toàn hệ thống thông tin của đơn vị;

c) Hướng dẫn, hỗ trợ người dùng tại đơn vị giải pháp phòng, chống vi rút máy tính. Thực hiện việc đánh giá, báo cáo các rủi ro và mức độ các rủi ro ảnh hưởng đến hoạt động hệ thống thông tin của đơn vị, các giải pháp cơ bản khắc phục các rủi ro;

d) Phối hợp với các các nhân, tổ chức có liên quan trong việc kiểm tra, phát hiện, phòng ngừa, đấu tranh, ngăn chặn xâm phạm an toàn, an ninh thông tin; tham gia khắc phục các sự cố mất an toàn, an ninh thông tin.

Điều 12. Trách nhiệm của các cơ quan Nhà nước trên địa bàn tỉnh

1. Cơ quan nhà nước có bị sự cố về an toàn thông tin, thực hiện theo nội dung quy định tại khoản 1 Điều 42 Nghị định số 64/2007/NĐ-CP.

2. Thực hiện báo cáo định kỳ hàng năm (trước ngày 15 tháng 10 hàng năm) đến Sở Thông tin và Truyền thông, theo mẫu hướng dẫn từ Sở Thông tin và Truyền thông, làm cơ

sở để Sở Thông tin và Truyền thông tổng hợp báo cáo UBND tỉnh và Bộ Thông tin và Truyền thông.

3. Tuân thủ và bảo đảm an toàn thông tin trong ứng dụng công nghệ thông tin theo quy định quy chế này và các quy định khác của pháp luật có liên quan.

4. Tuyên truyền, phổ biến quy chế này và các quy định khác của pháp luật có liên quan về an toàn thông tin trong phạm vi trách nhiệm và quyền hạn của từng cơ quan.

Điều 13. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu UBND tỉnh về công tác bảo đảm an toàn thông tin trên địa bàn tỉnh và phối hợp với các đơn vị có liên quan trong việc bảo đảm an toàn cho các hệ thống thông tin cấp tỉnh.

2. Xây dựng và triển khai các Kế hoạch, chương trình, dự án đầu tư, đào tạo về an toàn thông tin trong ứng dụng CNTT trên địa bàn tỉnh.

3. Tùy theo mức độ sự cố, phối hợp Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin trên địa bàn tỉnh; Cảnh báo các vấn đề về an toàn thông tin trong các cơ quan nhà nước trên địa bàn tỉnh.

4. Quản lý vận hành, hướng dẫn kết nối mạng truyền số liệu chuyên dùng của các cơ quan Đảng và nhà nước trên địa bàn tỉnh;

5. Hướng dẫn, hỗ trợ sao lưu dự phòng các thông tin, cơ sở dữ liệu của các cơ quan nhà nước một cách an toàn.

6. Hướng dẫn, giám sát các đơn vị xây dựng quy chế và thực hiện việc đảm bảo an toàn cho hệ thống thông tin theo quy định; Hướng dẫn các cơ quan về khung báo cáo; định kỳ tổng hợp báo cáo UBND tỉnh và Bộ Thông tin và Truyền thông về công tác an toàn thông tin số trên địa bàn tỉnh.

7. Tuyên truyền và định hướng tuyên truyền, phối hợp tuyên truyền đến các phương tiện truyền thông đại chúng trên địa bàn tỉnh về công tác bảo đảm an toàn, an ninh thông tin.

Điều 14. Trách nhiệm của Sở Tài chính

Hướng dẫn lập dự toán, quản lý, sử dụng và quyết toán kinh phí ngân sách nhà nước, thực hiện nhiệm vụ chuyên môn về bảo đảm an toàn, an ninh thông tin.

Điều 15. Trách nhiệm của Sở Kế hoạch và Đầu tư

Ưu tiên bố trí nguồn kinh phí đầu tư để thực hiện các dự án bảo đảm an toàn, an ninh thông tin.

Chương IV
CÔNG TÁC THANH TRA, KIỂM TRA, KHEN THƯỞNG VÀ XỬ LÝ VI PHẠM AN TOÀN THÔNG TIN SỐ

Điều 16. Thanh tra, kiểm tra

1. Các tổ chức, cá nhân tham gia vào quá trình ứng dụng công nghệ thông tin trên địa bàn tỉnh, chịu sự thanh tra, kiểm tra của các cơ quan Nhà nước có thẩm quyền về lĩnh vực an toàn thông tin.

2. Sở Thông tin và Truyền thông, Công an tỉnh phối hợp thường xuyên hoặc đột xuất kiểm tra, thanh tra về an toàn an ninh thông tin trong hoạt động ứng dụng CNTT trong cơ quan Nhà nước.

Điều 17. Xử lý vi phạm

Tổ chức, cá nhân có hành vi vi phạm các quy định về an toàn, an ninh thông tin trong ứng dụng công nghệ thông tin của cơ quan Nhà nước, tùy theo tính chất, mức độ vi phạm sẽ bị xử phạt vi phạm hành chính hoặc truy cứu trách nhiệm hình sự theo quy định của pháp luật.

Chương V
ĐIỀU KHOẢN THI HÀNH

Điều 18. Trách nhiệm thi hành

1. Sở Thông tin và Truyền thông chủ trì, phối hợp với các Sở, Ban ngành, UBND các huyện, thị xã, thành phố và các đơn vị có liên quan triển khai thực hiện Quy chế này.

2. Trong quá trình thực hiện nếu có phát sinh khó khăn, vướng mắc cần sửa đổi, bổ sung các cơ quan, đơn vị kịp thời báo cáo về Sở Thông tin và Truyền thông tổng hợp trình UBND tỉnh xem xét, quyết định./.

TM. ỦY BAN NHÂN DÂN TỈNH
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Hồ Việt Hiệp

PHỤ LỤC I

MẪU BIÊN BẢN SỰ CỐ AN TOÀN THÔNG TIN

(Ban hành kèm theo Quyết định số: /2013/QĐ-UBND ngày tháng năm 2013 của Ủy ban nhân dân tỉnh An Giang)

Đơn vị:
…….....
……
……
_____

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc
_____

……, Ngày tháng năm

- Họ và tên * .....
- Cơ quan * .....
- Email * .....
- Điện thoại * .....

1. Thông tin về sự cố:

- Mô tả sơ bộ về sự cố *.....
  .....
  .....
- Hình thức phát hiện * (*đánh dấu những cách thức được sử dụng để phát hiện sự cố)*
  ☐ Qua hệ thống IDS ☐ Kiểm tra Log File ☐ Quản trị hệ thống
  ☐ Khác, đó là .....
- Thời gian xảy ra sự cố *: …/… /……/…/… (ngày/tháng/năm/giờ/phút)

  (Ngày, tháng điền đủ 02 chữ số, năm điền đủ 04 chữ số ,giờ, phút điền đủ 02 chữ số theo hệ 24 giờ).
- Thời gian thực hiện báo cáo sự cố *: …/… /…/…(ngày/tháng/năm/giờ/phút)
- Các địa chỉ IP *(IP nội bộ (LAN) phát hiện hoặc bị phát hiện sự cố) (nếu có)*

2. Thông tin về hệ thống xảy ra sự cố:

- Hệ điều hành * ..... Version * .....
- Các dịch vụ có trên hệ thống (*đánh dấu những dịch vụ được sử dụng trên hệ thống)*
  ☐ Web server ☐ Mail server ☐ Database server

☐ FTP server ☐ Proxy server ☐ Application server

☐ Dịch vụ khác, đó là .....

- Các địa chỉ IP của hệ thống (*)

(Chỉ liệt kê các địa chỉ IP được sử dụng trên Internet, WAN; không cần liệt kê các địa chỉ IP nội bộ)

.....

.....

- Các tên miền của hệ thống (*)

.....

.....

- Mục đích chính sử dụng hệ thống (*) .....

.....

.....

Chú ý:

- *Phải điền đầy đủ thông tin trong những mục đánh dấu **
- *Ký và ghi đầy đủ họ tên, chức vụ (nếu có) vào cuối bản báo cáo.*

Người /Đơn vị lập biên bản

(Ký và ghi đủ họ tên)